



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,621	01/31/2002	John A. Copeland III	10775-36791	2472
7590	10/02/2006		EXAMINER BAUM, RONALD	
John R. Harris Morris, Manning & Martin, LLP 1600 Atlanta Financial Center 3343 Peachtree Rd., N.E. Atlanta, GA 30326			ART UNIT 2136	PAPER NUMBER

DATE MAILED: 10/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/062,621	COPELAND, JOHN A.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 01 February 2006.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-36 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>03302006</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 01 February 2006.
2. Claims 1- 36 are pending for examination.
3. Claims 1- 36 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –
(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1,4,9,10,14,17, 20 and 23-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Shipley, U.S. Patent 6,119,236.
5. As per claim 1; “A method for determining unauthorized usage of a data communications network, comprising the steps of:

monitoring packets exchanged between two hosts on the data communications network;
identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic;

storing information associating a service that is associated with an identified flow with at least one of the hosts that is associated with the identified flow, said service comprising an observed service [col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly

Art Unit: 2136

encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

determining if an observed service associated with a particular host is out of profile by comparing the service to a prestored allowed network services profile for the particular host [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

in response to determination that an observed service associated with a particular host is out of profile, providing an output indicating that the observed service is out of profile [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]".

As per claim 23, this claim is the apparatus/system for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

6. Claim 4 *additionally recites* the limitation that; "The method of claim 1, further comprising the steps of:

generating an alarm when an observed network service is not an allowed network service for the particular host.”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

7. As per claim 9; “A method for determining unauthorized usage of a data communications network, comprising the steps of:

monitoring packets exchanged between two hosts on the data communications network; identifying a flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined characteristic;

storing information associating a service that is associated with an identified flow with at least one of the hosts that is associated with the identified flow, said service comprising an observed service [col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such

Art Unit: 2136

collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.), as broadly interpreted by the examiner.];

determining hosts on the network that act as a client and server for each identified flow;

determining an allowed network services profile comprising information indicating particular network services that are authorized for use by each one of a plurality of hosts in a predefined group of hosts [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

generating an alarm in response to determination that an observed network service for a particular host in the group of hosts not included in the, allowed network services profile [col. 3,lines 17-col. 12,line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.”].”.

As per claim 17, this claim is the apparatus/system for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

8. As per claim 10, this claim is the “allowed network services port profile” variation for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner. Further, the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, also clearly encompassing the claimed limitations as broadly interpreted by the examiner. Still further, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), also clearly encompassing the claimed limitations as broadly interpreted by the examiner.

9. Claim 14 *additionally recites* the limitation that; “The method of claim 10, further comprising the step of
building the network services port profile based upon network service ports observed during a profile generation time period.”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

10. Claim 20 *additionally recites* the limitation that; “The system of claim 17, wherein the process is further operative to build the prestored network services profile based upon network services observed during a profile generation time period.”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

11. Claim 24 *additionally recites* a limitation dealing with predetermined characteristic options, inclusive of predetermined characteristics of traffic on a given port.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, whereas the Internet services observed (i.e., FTP, Internet network management error), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

12. Claim 25 ***additionally recites*** a limitation dealing with firewall communications in response to an alarm.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, and more particularly col. 9,lines 54-col. 10,line 35, as broadly interpreted by the examiner.).

13. Claim 26 ***additionally recites*** a limitation dealing with network administrator notification in response to an alarm.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, and more particularly col. 3,lines 22-62, as broadly interpreted by the examiner.).

14. Claim 27 ***additionally recites*** a limitation dealing with servicing the alarm via a utilization component inclusive of a firewall.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, and more particularly col. 9,lines 54-col. 10,line 35, as broadly interpreted by the examiner.).

Art Unit: 2136

15. Claim 28 *additionally recites* a limitation dealing with port number being a constant for plural packages for a single service.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the Internet services observed (i.e., FTP, Internet network management error) as related to the associated port numbers are fixed (i.e., WWW, email SMTP are typically a fixed port number), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

16. Claim 29 *additionally recites* a limitation dealing with a monitoring appliance performing the pertinent steps.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the INSD is a monitoring appliance, as broadly interpreted by the examiner.).

17. Claim 30 *additionally recites* a limitation dealing with a monitoring appliance performing the pertinent steps for hosts inside and outside the monitoring appliance.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on nodes locally and on the other side of the firewall, as broadly interpreted by the examiner.).

18. Claim 31 *additionally recites* a limitation dealing with the monitoring appliance coupled to a network device.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on network node devices locally and on the other side of the firewall, as broadly interpreted by the examiner.).

19. Claim 32 *additionally recites* a limitation dealing with the monitoring appliance coupled to a network device, inclusive of a router.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on network node devices locally and on the other side of the firewall such as routers inherent in the Internet configuration, as broadly interpreted by the examiner.).

20. Claim 33 *additionally recites* a limitation dealing with the monitoring appliance coupled to a network device, inclusive of a security device.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3, lines 17-col. 12, line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on network node devices locally and on the other side of the firewall such as routers inherent in the Internet configuration, of which said routers/bouters include security features (i.e., filtering, authentication features, etc.,), as broadly interpreted by the examiner.).

21. Claim 34 *additionally recites* a limitation dealing with the monitoring of packet headers. The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on network node devices locally and on the other side of the firewall such as routers inherent in the Internet configuration, of which said routers/brouters include security features (i.e., filtering, authentication features, etc.,) of which said filtering typically involves looking at the packet header information, as broadly interpreted by the examiner.).

22. Claim 35 *additionally recites* a limitation dealing with the unauthorized use from inside/outside addresses.

The teachings of Shipley suggest such limitations (figures 1-2 and associated descriptions, col. 3,lines 17-col. 12,line 35, whereas the INSD is a monitoring appliance that clearly communicates and operates on nodes locally and on the other side of the firewall (i.e., inside/outside addresses), as broadly interpreted by the examiner.).

23. Claim 36 *additionally recites* a limitation dealing with the flow service aspects.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

24. Claims 2,3,5 and 6-8 and 11-13,15,16 and 18,19,21,22 rejected under 35 U.S.C. 103(a) as being unpatentable over Shipley, U.S. Patent 6,119,236 as applied to claims 1,4,10,17, respectively, above, and further in view of Vaid et al, U.S. Patent 6,502,131 B1.

The teachings of Shipley suggest the base claims limitations (see “As per claim 1, ... As per claim 4, ...10, ...17” paragraphs above) *without explicitly teaching* of the use of “... displaying indicia ... observed network services ... monitoring period ...”, “... displaying indicia ... observed network services ... presentment period ...”, “... displaying indicia ... observed network services ... not an allowed ... service ...”, “...building [and] editing a network service [and block of network address] profile ... observed ... profile generation time ...”, and, “... displaying [and editing associated profile] indicia ... observed network service port ... present monitoring period [and included] ...”, as a response/react/alarm interface functionality.

Vaid et al, teaches of using/displaying indicia dealing with the various aspects of network traffic management, and associated setup of display criteria and displaying thereof, indicating traffic/traffic flow via the packet level/port/IP address objects rendered on said display/terminal device, implemented using various object oriented/GUI (see figures 1-19 and associated descriptions). The Vaid et al invention also clearly encompasses the security aspects associated

with the applicants network communications monitoring aspects insofar as it is inherent that in the process of quality of service monitoring per se, the loss of packets, bandwidth/latency aspects of traffic flow, and traffic profiles in of themselves deal with the security aspects of denial of service, and intrusion detection (i.e., denial of unauthorized access to a network through a gateway such as a firewall); clearly security aspects associated with the applicants claimed invention.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Shipley network security device and method for firewall control via packet flow monitoring/control, with the Vaid et al teachings of actual firewall/network gateway node directory enabled policy management tool for intelligent traffic management, in order to provide the firewall configuration and efficient control thereof, upon the Shipley network resulting control of said firewall.

Such motivation to combine would clearly encompass the need to allow comprehensive firewall configuration and efficient control in an intrusion detection/packet scanning environment for the network communications (i.e., Vaid et al col. 2,lines 46-col. 4,line 13).

Response to Amendment

25. As per applicant's argument concerning the lack of teaching by Shipley of a flow based methodology, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The claim language (i.e., independent claim 1) is not directed to "a flow based methodology" of an explicit nature, just implicitly in a broad sense. The fact that the specification deals more explicitly with the nature of "a flow based methodology" does not render the requirement that the claim language not deal with this aspect more succinctly; just that said claim language is looked at in light of the specification. Therefore, the "flow based methodology" aspects of Shipley, such as the INSD related code/pattern searching/analysis and associated value assignment to perceived attempted network security breaches, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that said reference does not render the claim language limitations patently distinct.

26. As per applicant's argument concerning the lack of teaching by Shipley of a flow based methodology applied to detecting unauthorized activity, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. As detailed above, the claim language (i.e., independent claim 1) is not directed to "a flow based methodology" of an explicit nature, just implicitly in a broad sense, which the applicant should note would include the "comparison aspects" and "pattern matching aspects" of the Shipley reference, as so claimed. Therefore, the "flow based methodology" aspects of Shipley, such as the knowing of various network configuration aspects does not teach away from the INSD related code/pattern

searching/analysis and associated value assignment to perceived attempted network security breaches, as being *broadly interpreted by the examiner*, such that said reference does not render the claim language limitations patently distinct.

27. As per applicant's argument concerning the lack of teaching by Shipley of a flow based methodology applied to detecting unauthorized activity, inclusive of allowed services at predetermined nodes, such that a subsequent alarm is generated, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. As detailed above, the claim language (i.e., independent claim 1) is not directed to "a flow based methodology" of an explicit nature, just implicitly in a broad sense, which the applicant should note would include the "look for known code ..." and "breach" aspects of the Shipley reference, as so claimed. Further, the INSD involves using header/port number parameters (a port number is basically a service with an address parameter, relative to a host) in the comparison to determine if a breach occurs. Therefore, the breach alarm/generation/port number comparison use aspects of Shipley, as being *broadly interpreted by the examiner*, such that said reference does not render the claim language limitations patently distinct.

28. As per applicant's argument concerning the lack of teaching by Vaid et al of the network security aspects applied to detecting unauthorized activity, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The Vaid et al "directory enabled policy management tool for intelligent traffic management" would clearly encompass the network security aspects of the claim limitations in that a primary rational for any

network management tool is for dealing with the various network security issues (i.e., authentication, filtering packets, etc.). Further, the “traffic classes” aspects of Vaid et al, as being *broadly interpreted by the examiner*, clearly would encompass the flow aspects of the applicant’s claims, in view of the “a flow based methodology” as detailed above.

29. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

30. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

**NASSER MOAZZAMI
PRIMARY EXAMINER**


9/13/06

